ABSTRACT

Method for effecting a chained key-issuing process over a finite group of points in which the discrete logarithm problem applies, wherein an issuing user (User$_i$), who possesses an issuing user public value (**U**$_i$) and an issuing user private key (x_i), provides to a successor user (User$_{(i+1)}$) a successor user public value (**U**$_{(i+1)}$) and a successor user private key ($x_{(i+1)}$), and where the issuing user, except for a Certifying Authority (CA), was a successor user in a preceding step in the chained key-issuing process, and where the Certifying Authority acts as the first issuing user in the chained key-issuing process.

09615956.032201